



TITLE:

楕円曲線 $y^2 = x^3 - kx$ のrankに関して(代数的整数論)

AUTHOR(S):

長尾, 孝一

CITATION:

長尾, 孝一. 楕円曲線 $y^2 = x^3 - kx$ のrankに関して(代数的整数論). 数理解析研究所講究録 1991, 759: 168-179

ISSUE DATE:

1991-06

URL:

<http://hdl.handle.net/2433/82186>

RIGHT:

楕円曲線 $y^2 = x^3 - kx$ の rank に関して。

大阪大理学部 長尾孝一 (Koh-ichi Nagao)

§ 0. 序. 有理数体 \mathbb{Q} 上定義された楕円曲線の rank については数多くの研究がある。ここで楕円曲線の有理点の作る群の rank を単に rank ということにする。定義式が $y^2 = x^3 + k$ の形をしている場合には, 木原[1], 中野[2], Quer[3] 等の研究があり, rank ≥ 6 の曲線の無限個の存在([1], [2]) および rank = 12 の例([3]) が知られている。

ここでは定義式が $E_k: y^2 = x^3 - kx$ の形をしている \mathbb{Q} 上定義された楕円曲線について考察し 次の結果を得た。

Theorem 1 楕円曲線 E_k で rank ≥ 4 のものが (\mathbb{Q} 同型を除いて) 無限個存在する。

Theorem 2 $k_1 = 631^4 + 222^4 = 558^4 + 503^4$,
 $k_2 = 1203^4 + 76^4 = 1176^4 + 653^4$ とせよ。このとき,
 (1)

E_{R_1} と E_{R_2} は \mathbb{Q} 同型でなく, $\text{rank} \geq 5$ である。

以下で 2.1 の定理のアイデアをまとめてみる。

$$a(T) = (2T^7 + T^6 + 20T^5 - 17T^4 + 2T^3 - 17T^2 + 8T + 1) / 64$$

$$b(T) = (T^7 - 8T^6 - 17T^5 - 2T^4 - 17T^3 - 20T^2 + T - 2) / 64$$

$$c(T) = (2T^7 - T^6 + 20T^5 + 17T^4 + 2T^3 + 17T^2 + 8T - 1) / 64$$

$$d(T) = -(T^7 + 8T^6 - 17T^5 + 2T^4 - 17T^3 + 20T^2 + T + 2) / 64$$

を有理関数体 $\mathbb{Q}(T)$ の元とすると, 等式

$$a(T)^4 + b(T)^4 = c(T)^4 + d(T)^4 \text{ が成立する [4]。}$$

$R(T) = a^4(T) + b^4(T)$ とおき, $\mathbb{Q}(T)$ 上定義された楕円曲線

$\mathcal{E}: y^2 = x^3 - R(T)x$ を考える。このとき $\mathbb{Q}(T)$ 有理点

$$P_1 = (-a^2(T), a(T)b^2(T))$$

$$P_2 = (-b^2(T), b(T)a^2(T))$$

$$P_3 = (-c^2(T), c(T)d^2(T))$$

$$P_4 = (-d^2(T), d(T)c^2(T))$$

は \mathcal{E} 上の点となり, §2 の Proposition 2-1 にあって $\{P_i\}_{i=1,2,3,4}$

は \mathcal{E} 上で独立な点であることが示される。又, \mathcal{E} および

$\{P_i\}_{i=1,2,3,4}$ の変数 T に有理数 t を代入して得られる \mathbb{Q} 上定義された楕円曲線およびその有理点を $E_{R(t)}$ および $\{P_i(t)\}$

$i=1,2,3,4$ と書くと, Silvermann の特殊化定理 (Lemma 2-1) によ

て ほとんどすべての有理数 t に対して $\{P_i(t)\}_{i=1,2,3,4}$ は

(2)

$E_{\mathbb{R}(t)}$ 上独立な点であることがわかる。

§1 2 isogeny. ここでは $E_{\mathbb{R}}$ の rank の計算の準備として 2 isogeny による descent の方法をまとめてみる ([5] §X)。
 簡単のために $E = E_{\mathbb{R}}$ $E' = E_{-4\mathbb{R}}$ ($\mathbb{R} \in \mathbb{Z}$) とおく。このとき E と E' は 2 isogeny $\phi: E \rightarrow E'$, $\phi(x, y) = (y^2/x^2, -(R+x)y/x^2)$ およびその相対 $\phi': E' \rightarrow E$, $\phi'(x, y) = (y^2/4x^2, (4R-x^2)y/8x^2)$ によって 2 isogenous である。(このとき ϕ および ϕ' の kernel はそれぞれ $E[\phi] = \{O, (0,0)\}$, $E'[\phi'] = \{O, (0,0)\}$ である。) 次に $\delta: E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ および $\delta': E'(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ を次で定義される写像とする。

$$\delta(P) = \begin{cases} [x] & P = (x, y), x \neq 0, \infty \text{ のとき} \\ [1] & P = O \text{ のとき} \\ [-R] & P = (0, 0) \text{ のとき} \end{cases}$$

$$\delta'(P') = \begin{cases} [x] & P' = (x, y), x \neq 0, \infty \text{ のとき} \\ [1] & P' = O \text{ のとき} \\ [R] & P' = (0, 0) \text{ のとき} \end{cases} \quad (1-1)$$

ここで $[a]$ は有理数 a で代表される $\mathbb{Q}^*/\mathbb{Q}^{*2}$ の元である。
 以下では有理数 a と $\mathbb{Q}^*/\mathbb{Q}^{*2}$ の元 $[a]$ を簡単のため同一視する。
 このとき δ および δ' は準同形写像で、

$\ker \delta = \phi'(E'(\mathbb{Q}))$, $\ker \delta' = \phi(E(\mathbb{Q}))$ である ([5] 301 p Exmpl 4.8)。

よって写像 δ および δ' は 次の様な群の埋め込みとみなすことができる。

$$\left. \begin{array}{l} \delta: E(\mathbb{Q})/\phi'(E'(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \\ \delta': E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \end{array} \right\} (1-2)$$

以下 E の有理 2-torsion $E(\mathbb{Q})[2]$ が $\{O, (0,0)\}$ である

と仮定する。 $\phi \circ \phi' = 2$ であるので 次の完全列が成

り立つ ([5] 301 p remark 4.7)。

$$\begin{array}{c} 0 \rightarrow \{O, (0,0)\} \rightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\phi'} \\ E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow E(\mathbb{Q})/\phi'(E'(\mathbb{Q})) \rightarrow 0 \end{array} \left. \vphantom{\begin{array}{c} 0 \rightarrow \{O, (0,0)\} \rightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\phi'} \\ E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow E(\mathbb{Q})/\phi'(E'(\mathbb{Q})) \rightarrow 0 \end{array}} \right\} (1-3)$$

E の有理点 P に対して E' の有理点 P' を $\phi'(P') = P$ を満たす点 (必ずしも有理点とは限らない) とする。

(1-3) が完全列であることにより, 次の Lemma が得られる。

又, この Lemma は P' のとり方に依らないことを先に注意しておく。

Lemma 1-1 (1) $P' \in E'(\mathbb{Q}) \iff \delta(P) = 1$ 。

(2) $P \in 2E(\mathbb{Q}) \iff P' \in E'(\mathbb{Q})$ が $\delta'(P') = 1$ 。

§2 Theorem 1 の証明

Proposition 2-1 $\{P_i\}_{i=1, \dots, 4}$ は E 上で独立な点である。
(4)

証明) ある有理数 t について $\{P_i(t)\}_{i=1, \dots, 4}$ が $E_{\mathbb{R}(t)}$ 上で独立な点であることを示せば、この Proposition が得られるので、以下 $\{P_i(3)\}_{i=1, \dots, 4}$ が $E_{\mathbb{R}(3)}$ 上で独立な点であることを証明する。簡単のために $\mathbb{R} = \mathbb{R}(3)$, $P_i = P_i(3)$ ($i=1, \dots, 4$), $E = E_{\mathbb{R}(3)}$ $E' = E_{-4\mathbb{R}(3)}$ とおく。直接計算することによって

$$\mathbb{R} = 41 \times 113 \times 241 \times 569$$

$$P_1 = (-a^2, ab^2)$$

$$P_2 = (-b^2, ba^2)$$

$$P_3 = (-c^2, cd^2)$$

$$P_4 = (-d^2, dc^2)$$

$$(a, b, c, d) = (133, -134, 158, 59) \text{ を得る。}$$

ここで、 a および $-4\mathbb{R}$ が非平方数であるので、 $E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})[2] = \{O, (0,0)\}$ が成立し ([5] 311 p Prop 6.1), § 1 の仮定 ($E(\mathbb{Q})[2] = \{O, (0,0)\}$) が成立している。さらに計算することによって

$$P_1 + P_2 = (3^2 \cdot 13^2 \cdot 457^2, -2^6 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 67 \cdot 457 \cdot 557)$$

$$P_1 + P_3 = (11^2 \cdot 89^2 / 3^2, -2^3 \cdot 11 \cdot 43 \cdot 89 \cdot 2707 / 3^3)$$

$$P_1 + P_2 + P_3 + P_4 = ((884309822379 / 5108208264)^2, *)$$

および $\delta(P_1 + P_2) = \delta(P_1 + P_3) = \delta(P_1 + P_2 + P_3 + P_4) = 1$ を得る。

Lemma 1-1 (1) より $E'(\mathbb{Q})$ の元 P', Q', R' で $\phi'(P') = P_1 + P_2$,

$\phi'(Q') = P_1 + P_3$, $\phi'(R') = P_1 + P_2 + P_3 + P_4$ を満たすものが存在

する。実際 P', Q', R' として

(5)

$$P' = (2, -2^2 \cdot 3 \cdot 13 \cdot 457)$$

$$Q' = (2 \cdot 3^2 \cdot 41 \cdot 569, 2^2 \cdot 3 \cdot 11 \cdot 41 \cdot 89 \cdot 569)$$

$$R' = (53^2 \cdot 12281^2 / 2^4 3^4 109^2, \quad *)$$

とすると これは上記の性質を満たし

$$\delta'(P') = 2, \quad \delta'(Q') = 2 \cdot 41 \cdot 569, \quad \delta'(R') = 1 \quad \text{が成り立つ。すると}$$

Lemma 1-1(2)より $P_1 + P_2 + P_3 + P_4 \in 2E(\mathbb{Q})$ が得られる。

$$\text{実際 } P_5 = (241 \cdot 569, 2^2 \cdot 7 \cdot 13 \cdot 241 \cdot 569)$$

とあくと, $P_1 + P_2 + P_3 + P_4 = 2P_5$ が成り立つ。

以下 $\{P_i\}_{i=1,2,3,4}$ の E 上の独立性を示す代りに

$\{P_i\}_{i=1,2,3,5}$ の独立性を証明する。 $\{P_i\}_{i=1,2,3,5}$ が独立

であると仮定する。すると 整数 m_1, m_2, m_3, m_5 で

$$\gcd(m_1, m_2, m_3, m_5) = 1, \quad \text{および}$$

$$m_1 P_1 + m_2 P_2 + m_3 P_3 + m_5 P_5 \in E(\mathbb{Q})_{\text{tors}} = \langle (0,0) \rangle$$

を満たすものが存在することが簡単にわかる。この式を

どうつすことにより

$$\begin{aligned} \langle -41 \cdot 113 \cdot 241 \cdot 569 \rangle &\ni \delta(m_1 P_1 + m_2 P_2 + m_3 P_3 + m_5 P_5) \\ &= \delta(P_1)^{m_1} \cdot \delta(P_2)^{m_2} \cdot \delta(P_3)^{m_3} \cdot \delta(P_5)^{m_5} \\ &= (-1)^{m_1 + m_2 + m_3} (241 \cdot 569)^{m_5} \pmod{\mathbb{Q}^{\times 2}} \end{aligned}$$

を得, $m_1 + m_2 + m_3, m_5 \in 2\mathbb{Z}$ かつ $m_2(P_1 + P_2) + m_3(P_1 + P_3) \in 2E(\mathbb{Q})$ (*)

を得る。 Lemma 1-1(1) かつ (*) より, $E'(\mathbb{Q})$ の元 S' で

$$\phi'(S') = m_2(P_1 + P_2) + m_3(P_1 + P_3) \text{ を満たすものの存在がわかり}$$

(6)

ϕ' が準同型写像であることより $S' = m_2 P' + m_3 Q'$ を得る。

この式の両辺を δ' でうつし Lemma 1-1 (2) を使うと

$$\begin{aligned} \langle 41 \cdot 113 \cdot 241 \cdot 569 \rangle &\equiv \delta'(m_2 P' + m_3 Q') \\ &= 2^{m_2} \cdot (2 \cdot 41 \cdot 569)^{m_3} \pmod{\mathbb{Q}^{x^2}} \end{aligned}$$

を得, $m_2, m_3 \in \mathbb{Z}$ を得る。これは $\gcd(m_1, m_2, m_3, m_5) = 1$ に矛盾するので この Proposition は証明された。

Lemma 2-1 (Silvermann の特殊化定理 [5] 368p Th20.3)

C を代数体 K 上定義された曲線, E を C の関数体 $K(C)$ 上定義された楕円曲線とする。このとき 有限個を除いた C の K -有理点 t に対して 特殊化写像

$$\phi_t: E(K(C)) \longrightarrow E_t$$

は定義され injective である。

この Lemma と Proposition 2-1 より次の Proposition がわかる。

Proposition 2-2 ほとんどすべての有理数 t に対して

$\{P_i(t)\}_{i=1 \sim 4}$ は $E_{\mathbb{R}}(t)$ 上で独立な点である。

Theorem 1 の証明を完成するためには楕円曲線の族 $\{E_{\mathbb{R}}(t) \mid t \in \mathbb{Q}\}$ が互いに \mathbb{Q} -同型でない曲線を無限個含むことを言えばよい。

E_{k_1} と E_{k_2} ($k_1, k_2 \in \mathbb{Q}^*$) が \mathbb{Q} -同型である必要十分条件は $k_1/k_2 \in \mathbb{Q}^{*4}$ とかけれる ([5], 303p Cor. 5.4.1) ので, これは次の Proposition に帰着される。

Proposition 2-3 $k(T)$ を $\{0\}$ で定義された T の多項式とし,

$C: k S^4 = k(T)$ ($k \in \mathbb{Q}^*$) を (S, T) plane 上の affine curve とする。このとき C は有理点を高々有限個しか含まない。

証明 (概略), 曲線 C の genus は 39 であり, Faltings によって証明された Mordell 予想 [9] によって C は高々有限個しか有理点を含まないことがわかる。

§3 Theorem 2 の証明

Lemma 3-1 ([5] 302p Prop 4.9)

k, d を 0 でない整数とし, C'_d を定義式 $dW^2 = d^2Z^4 - k$ で定義される (W, Z) plane 内の曲線とする。

(1) E_k が \mathcal{O} および $(0,0)$ でない有理点 P で $\delta(P) = d$ を満たすものを含む必要十分条件は C'_d が Z 座標が 0 でない有理点を含まることである。

(2) $(w_0, z_0) \in C'_d(\mathbb{Q})$ とせよ。このとき $(d z_0^2, d w_0 z_0) \in E_k(\mathbb{Q})$ が成り立つ。
(8)

この Lemma を Theorem 2 で登場した曲線 E_{k_1} に適応する。

簡単の為 $E = E_{k_1}$, $E' = E_{-4k_1}$ とおく。直接計算することにより

$$(253009, 558) \in C'_{-1}(\mathbb{Q})$$

$$(21993/4, 19/2) \in C'_{6673}(\mathbb{Q})$$

$$(4856/9, 1/3) \in C'_{17 \cdot 257 \cdot 5521}(\mathbb{Q})$$

が得られ、Lemma 3-1(2) より 有理点

$$P_1 = (-311364, -141179022)$$

$$P_2 = (2408953/4, 2788426491/8)$$

$$P_3 = (24121249/9, 117132785144/27)$$

で $\delta(P_1) = -1$, $\delta(P_2) = 6673$, $\delta(P_3) = 17 \cdot 257 \cdot 5521$ を満たす点

が E 上にあることがわかる。よって, (1-2) の埋め込み

$$\text{より } E(\mathbb{Q})/\phi'(E'(\mathbb{Q})) \cong \delta(E(\mathbb{Q})/\phi'(E'(\mathbb{Q})))$$

$$\supset \langle \delta(P_1), \delta(P_2), \delta(P_3) \rangle$$

$$= \langle -1, 6673, 17 \cdot 257 \cdot 5521 \rangle$$

および $\dim_{\mathbb{Z}/2\mathbb{Z}} (E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))) \geq 3$ を得る。

同様に Lemma 3-1 を曲線 E' に適応することによって

$$\text{有理点 } P'_1 = (6050, 62413780)$$

$$P'_2 = (246977/4, 1599781567/8)$$

$$P'_3 = (195024, 1007162904)$$

$$P'_4 = (5558609/16, 32983991719/64)$$

(9)

$$\delta'(P'_1) = 2, \quad \delta'(P'_2) = 257, \quad \delta'(P'_3) = 5521, \quad \delta'(P'_4) = 17.6673$$

を満たす点 \mathcal{E} 上にあることがわかり、前と同様に

$$\dim_{\mathbb{Z}/2\mathbb{Z}} (E'(\mathcal{Q})/\phi(E(\mathcal{Q}))) \geq 4 \quad \text{を得る。}$$

ここで \mathcal{R}_1 および $-4\mathcal{R}_1$ が非平方数であるので

$$E(\mathcal{Q})_{\text{tor}} = E(\mathcal{Q})[2] = \{O, (0,0)\} \quad \text{が成り立ち、完全列 (1-3) が成立}$$

する。完全列 (1-3) と $E(\mathcal{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z}$ より 次の等式が成立する。

$$\begin{aligned} \text{rank } E(\mathcal{Q}) &= \dim_{\mathbb{Z}/2\mathbb{Z}} (E(\mathcal{Q})/2E(\mathcal{Q})) - 1 \\ &= \dim_{\mathbb{Z}/2\mathbb{Z}} (E(\mathcal{Q})/\phi'(E(\mathcal{Q}))) + \dim_{\mathbb{Z}/2\mathbb{Z}} (E'(\mathcal{Q})/\phi(E(\mathcal{Q}))) - 2 \\ &\geq 3 + 4 - 2 = 5. \end{aligned}$$

同様に $\text{rank } E\mathcal{R}_2 \geq 5$ も証明できる。

Appendix 広島大学の小池先生から次の様な興味深い注意をいただいた。

$$A, B, C, D \text{ を関係式 } A^4 + D^4 = 2(B^4 + C^4)$$

$$\text{をみたす自然数とし } h = -(A^8 + B^8 + C^8 - 2A^4B^4 - 2A^4C^4 - 2B^4C^4)/2^6 3^4$$

と置く。このとき 有理数

$$R_1 = (A^2 B^2 / 2^2 3^2, AB(A^4 + B^4 - C^4) / 2^4 3^3)$$

$$R_2 = (A^2 C^2 / 2^2 3^2, AC(A^4 + C^4 - B^4) / 2^4 3^3)$$

$$R_3 = (B^2 C^2 / 2^2 3^2, BC(B^4 + C^4 - A^4) / 2^4 3^3)$$

$$R_4 = (D^2 B^2 / 2^2 3^2, DB(D^4 + B^4 - C^4) / 2^4 3^3)$$

$$R_5 = (D^2 C^2 / 2^2 3^2, DC(D^4 + C^4 - B^4) / 2^4 3^3)$$

(10)

は E_h 上にある。特に $(A, B, C, D) = (21, 20, 7, 19)$ のとき、
楕円曲線 E_h ($h = 2^2 \cdot 5^2 \cdot 11 \cdot 89$) が得られ、又 E_h の rank
が 4 であることが Silverman の教科書の例 ([5], 303 p Example 4.10)
と同様に証明できる。

\$\$\$ Reference

- [1] S.Kihara:On the rank of the elliptic curve $y^2 = x^3 + k$. Proc.Japan Acad.63,Ser. A(1978) 76-78.
- [2] S.Nakano:Construction of pure cubic fields with large 2-class groups. Osaka J.Math.25(1988),161-170.
- [3] J.Quer:Corps quadratiques des 3rang 6 et courbes elliptiques de rang 12 C.R Acad,Sci.Paris.305,Serie 1,(1987), 215-218.
- [4] L.J.Lander and T.R.Parkin:Equal sums of biquadrates. Math Comp.20,(1966) 450-451.
- [5] J.H.Silverman:The arithmetic of elliptic curves, Graduate Texts in Math.106,Springer-Verlag,New-York,1986.
- [6] B.Birch and H.P.F.Swinnerton-Dyer:Note on elliptic curves (I) and (II) J.Reine Angew.Math.212(1963)7-25 and 218(1965),7-108.
- [7] A.C.Hearn:Reduce User's Manual,The Rand corporation,Santa Monica,1987.
- [8] Miyaji:On the rank of Elliptic curve,Master thesis in Osaka University (1989).
- [9] G.Faltings:Endlichkeitssatze fur abelsche varietaten uber Zahlenkorpern, Invent Math.73,349-366